SUBJECT: Fraudulent Activity Targeting Purchase and Travel Cardholders

DATE: Mon, 9 Feb 2004 10:47:16 -0500

FROM: broadcast@doc.gov

FOR: All DOC Employees Who Have Ben Issued a Government Purchase or Travel Card

Recently there have been several reports of external fraudulent activity targeted toward or affecting the government's charge card program. Below are two examples of this activity, and instructions for reporting any incidences:

1. Do not give out account information in response to a fraudulent e-mail indicating it is from Visa officials stating that cardholders have to "reactivate" their accounts due to a "technical security update." The e-mail directs the user to click a link that appears to be the Visa Web site, but is actually a fake mirror image. Entering personal information into that site could result in identity theft. Note that no one from Visa banks will ever call or e-mail a cardholder and ask for an account number or other personal information. Thus far, this action has been targeted at government travel cardholders.

2. Information also warns of a potential scam whereas unknown callers falsely identify themselves as bank employees working with the government charge card program. The scam operators claim to be checking suspicious card activity and may ask for account numbers, social security numbers, and other personal information. Be aware that bank employees would not take these actions. Agency/Organization Program Coordinators (A/OPCs) should be the only persons requesting this type of information.

Cardholders should report any of these fraudulent attempts to collect information to their A/OPC and to Citibank at 1-800-790-7206 as soon as they occur. If you are unsure of who your A/OPC is, contact the Commerce Bankcard Center at (816) 823-3847.

This message is authorized by OAM and OAS.